EFFECTIVENESS OF DIGITAL FORENSIC EVIDENCE IN CRIMINAL TRIAL: AN EMPIRICAL STUDY WITH SPECIAL REFERENCE TO RAJASTHAN

Synopsis of the Research Proposal

Submitted for the Registration in the

Ph.D Programme (Part-Time) in Law

Submitted by:

Niharika Kumari

(Enrollment Number- 25JPPHNDLS003)

Under Supervision of

Dr. Ameesha Singh

Assistant Professor

ICFAI Law School

The ICFAI University, Jaipur

EFFECTIVENESS OF DIGITAL FORENSIC EVIDENCE IN CRIMINAL TRIAL: AN EMPIRICAL STUDY WITH SPECIAL REFERENCE TO RAJASTHAN

Synopsis of the Research Proposal

Submitted for the Registration in the

Ph.D Programme (Part-Time) in Law

Submitted by:

Niharika Kumari

(Enrollment Number - 25JPPHNDLS003)

Under Supervision of

Dr. Ameesha Singh

Assistant Professor

Ms. Niharika Kumari — **Research Scholar**

Dr. Ameesha Singh — **Supervisor**

ICFAI Law School

The ICFAI University, Jaipur

TABLE OF CONTENTS

S. No.	Particulars	Page No.
1.	LIST OF ABBREVIATIONS	3
2.	LIST OF CASES	4
3.	ABSTRACT	5
4.	INTRODUCTION	6
5.	REVIEW OF LITERATURE	14
6.	RESEARCH GAPS	21
7.	STATEMENT OF THE RESEARCH PROBLEM	21
8.	SIGNIFICANCE OF THE STUDY	22
9.	RESEARCH OBJECTIVES	22
10.	RESEARCH QUESTIONS	23
11.	RESEARCH HYPOTHESES	23
12.	RESEARCH METHODOLOGY	24
13.	SCOPE AND LIMITATIONS OF THE STUDY	25- 26
14.	EXPECTED OUTCOMES	26
15.	RESEARCH TIMELINE	26
16.	BIBLIOGRAPHY	27

LIST OF ABBREVIATIONS

❖ Art.	Article
❖ BSA	Bharatiya Sakshya Adhiniyam, 2023
❖ CCTV	Closed-Circuit Television
❖ CJEU	Court of Justice of the European Union
❖ DNA	Deoxyribonucleic Acid
❖ ESI	Electronically Stored Information
❖ EU	European Union
❖ GDPR	General Data Protection Regulation
❖ IoT	Internet of Things
❖ IT	Information Technology
❖ NCRB	National Crime Records Bureau
❖ No.	Number
❖ SCC	Supreme Court Cases
❖ Sec.	Section
❖ SPSS	Statistical Package for the Social Sciences
❖ U.S.	United States
❖ V.	Versus

LIST OF CASES

1. Amitabh Bagchi v. Ena Bagchi, 2019 SCC OnLine Del 9487
2. Bundesrepublik Deutschland v. SpaceNet AG, ECLI:EU:C:2022:702
3. Carpenter v. United States, 585 U.S. 296 (2018)
4. Central Bureau of Investigation v. Ramesh Gelli, (2016) 3 SCC 788
5. Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559
6. La Quadrature du Net v. France, ECLI:EU:C:2020:791
7. Ministerio Fiscal, ECLI:EU:C:2018:788.Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
8. Nitesh Sheth v. State of Maharashtra, 2021 SCC OnLine Bom 3536
9. Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, ECLI:EU:C:2020:790
10. Prokuratuur v. H.K., ECLI:EU:C:2021:152
11. Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke, (2015) 3 SCC 123.
12. State of Karnataka v. M. R. Hiremath, (2019) 7 SCC 515
13. United States v. Chavez, 951 F.3d 349 (6th Cir. 2019)
14. United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020)
15. United States v. Miller, 589 F. Supp. 3d 60 (D.D.C. 2022)
16. United States v. Smith, 967 F.3d 1196 (11th Cir. 2020)
17. Van Buren v. United States, 593 U.S. 374 (2021)
18. Vibhor Garg v. Neha, 2022 SCC OnLine P&H 1087

TITLE

"Effectiveness of Digital Forensic Evidence in Criminal Trial: An Empirical Study with Special Reference to Rajasthan"

ABSTRACT

The digital transformation of society has impacted the way investigations are conducted. Digital evidence has emerged to be an important aspect of contemporary investigations. In India, especially in Rajasthan, the prolific use of mobile phones, digital payments, monitoring systems, and internet communication, has led to a corresponding increase in number of digital footprints linked to a crime. This means security agencies have to resort to digital evidence such as phone records, footage from CCTV, social media and cloud storage to conduct their investigations. The use of digital evidence introduces problems with the legality, reliability and privacy of people.

This research provides an exhaustive study of the current legislations, rules and guidelines related to digital evidence in a criminal case with particular reference to the state of Rajasthan. It evaluates the effectiveness of digital evidence in conjunction with the traditional evidence; it covers the authenticity, integrity and chain of custody. The research combines qualitative and quantitative techniques, including doctrinal legal techniques and fieldwork, to collect data from legal and forensic practitioners in Rajasthan. Additionally, it compares and contrasts the legal systems of India with those of the US and the European Union, to help in identifying the ideal systems. This study seeks to enhance the legal structure that governs evidence to ensure that the right to privacy is protected, while also facilitating the prosecution of criminals.

Keywords: Digital Forensic Evidence, Admissibility of Electronic Evidence, Criminal Trials, Digital Privacy, Comparative Criminal Procedure, Forensic Investigation

1. INTRODUCTION:

With all recent changes to society, criminals and criminal investigations are likely to change as well. Most criminal interactions happen via digital devices and software, including phones, laptops, servers, and cloud platforms. This means many criminals are creating digital footprints in the form of emails, metadata, call detail records, social media, communications, and cloud documents. Digital devices are creating evidence for criminal trials, and these new tools from law enforcement change the entire nature of legal investigations and analysis.[1]

Criminal digital evidence is created through legally sanctioned digital evidence retrieval techniques. Digital evidence includes mobile device records, voice and video recordings from closed circuit television systems, the history of Internet usage, logs of crypto currency block chain transactions, records of GPS navigation, and other types of digital communications. In modern criminal investigations, digital evidence usually is the main evidence and sometimes the only evidence in support of the guilt or innocence of the defendants.

In the past decade, the use of digital evidence during investigation of crimes has increased considerably in India. As the degree of use of smartphones, digital payment systems, and social media has increased, so has the reliance of investigative bodies on digital data, and digitally reconstructed records of the commission of crimes. This trend has raised significant and serious concerns regarding the digital data's legal and evidential concerns during the course of the investigation.[2]

In recent years, the state of Rajasthan has witnessed a significant transformation in the nature of criminal activity, driven largely by the rapid expansion of digital technologies. With an ever-growing number of smartphones, an expanding network of internet users and the rising popularity of digital financial platforms, cyber-fraud, identity theft, financial fraud, and digital harassment are all on the rise. Cities like Jaipur, Jodhpur and Udaipur have become important digital hubs, which has led to an increase in opportunities to improve technology and risks to cybercrime. Consequently, electronic evidence, or digital

[1] Dr. Muhammad Ramzan, "Forensic and Digital Evidence be used as Substantial Evidence in Criminal Cases, an Effective Alternative of Ocular Account: Evaluation in the Light of New Amendments. What are the Requirements of Admissibility and Reliability of Digital and Forensic Evidence?" 2022 *SSRN Elec. J.*, https://doi.org/10.2139/ssrn.4021315.
[2] *Id.*

evidence, which includes electronic records, logs of communications, surveillance videos, and metadata, is increasingly a critical element in criminal investigations throughout the state.

While digital evidence is increasingly a component of the criminal justice system in Rajasthan, there are still major issues concerning its admissibility, reliability, and adherence to constitutional safeguards for privacy rights. The state's investigative agencies may experience problems with the availability of the necessary forensic infrastructure, procedures that vary among agencies, and poor technical skills in the examination of electronic evidence. In addition, there are significant issues concerning the evidentiary standards for digital records in the state's system of justice that were raised with the implementation of recent changes in the law, such as the BSA 2023. Against this backdrop, an empirical and doctrinal study of the state of Rajasthan is necessary to comprehend the current use of digital forensic evidence and the need to strengthen the legal protections to ensure that effective law enforcement does not intrude upon individuals' rights.[3]

The legal considerations regarding digital evidence in India have undergone significant changes after BSA, 2023, was implemented, which repealed the prior evidence statutes regarding documents and electronic evidence. This newly enacted evidence law acknowledges the authenticity and reliability of ESI in evidence & procedural safeguards set forth to preserve that reliability. In that regard as to ESI, Sec. 63 & 65 that address the admissibility of ESI & certification of ESI continue to advance the legal and evidential concepts of ESI enunciated in the earlier Indian Supreme Court decisions on evidence.

Consequently, use of digital forensic evidence in criminal trials requires a balance between effective prosecution of crime and safeguarding privacy. The courts should prove the digital evidence to be both reliable and legally warranted. The absence of balancing these factors will wane the public’s confidence in the criminal justice system.

The last couple of years have shown the Indian judiciary showing confidence in using digital evidence when it comes to criminal prosecutions and investigations. Authenticity of digital evidence, Private and evidentiary issues surrounding electronic records have been

[3] Dr. John Varghese, “Electronic form evidence under the Bharatiya Sakshya Adhiniyam, 2023” 2024 *SSRN Elec. J.*, https://doi.org/10.2139/ssrn.4869744.

evolving. In "*State of Karnataka v. M R Hiremath",*[4] court stated that digital records are to be proven authentic in order to be relied upon. In "*Amitabh Bagchi v. Ena Bagchi",*[5] court stated that communication that was electronic and in recorded form are to be taken as evidence as long as, proven authentic. In "*Vibhor Garg v. Neha",*[6] court, when set to decide the case of the admissibility of interception of private communication, stated that recording of private communication, of course, would be taken as evidence as long as it is proven authentic. Similarly, in "*Nitesh Sheth v. State of Maharashtra",*[7] court held that the electronic form of communication, of one recorded, was taken to form the basis of proving criminal liability. In "*Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke",*[8] court held that electronic evidence in the form of recording conversations was taken as corroborative evidence. In "*Central Bureau of Investigation v. Ramesh Gelli",*[9] the importance of recording and evidence of electronic banking transactions and digital trail in proving offences of a financial nature is also evident. In a nutshell, such decisions of the Indian judiciary demonstrate the evolving nature of criminal law and the evidentiary value of electronic and digital evidence.

The USA has a vast range of case law regarding the constitutional regulation/ admissibility of digital evidence. For example, in "*Carpenter v. USA"*[10] the US's apex court held that data that reveals the historical location of a cellphone cannot be accessed without a warrant. Also, in "*Van Buren v. USA",*[11] court discussed the meaning of unauthorized access and its effect on digital investigations. Court in "*USA v. Smith"*[12] dealt with issues regarding the authentication of electronic communications (SMS, texts, and social media) and in *USA v. Chavez,*[13] court conversely underlined the importance of digital evidence and its reliability and chain of custody. Also in "*USA v. Gratkowski",*[14] the court discussed the privacy protection that participants have in relation to the block chain and crypto currency transactions. Lastly, "*USA v. Miller"*[15] case dealt with the evidentiary value of digital metadata, electronic communications and the criminal law. All these cases reflect

[4] (2019) 7 SCC 515
[5] 2019 SCC OnLine Del 9487
[6] 2022 SCC OnLine P&H 1087
[7] 2021 SCC OnLine Bom 3536
[8] (2015) 3 SCC 123
[9] (2016) 3 SCC 788
[10] 585 U.S. 296 (2018)
[11] 593 U.S. 374 (2021)
[12] 967 F.3d 1196 (11th Cir. 2020)
[13] 951 F.3d 349 (6th Cir. 2019)
[14] 964 F.3d 307 (5th Cir. 2020)
[15] 589 F. Supp. 3d 60 (D.D.C. 2022)

the struggle in the USA to find an equilibrium between the speed of constitutionally regulated investigations and the protection of digital data. In "*HiQ Labs, Inc. v. LinkedIn Corp.*",[16] court addressed scraping of publicly available data from LinkedIn. It held that accessing public digital data may not violate anti-hacking laws, raising important questions about ownership and forensic use of online information. In "*United States v. Ganias*"[17], the issue concerned the retention of mirror images of hard drives seized during investigation. The Court held that indefinite retention and later use of unrelated data may violate the Fourth Amendment, emphasizing limits on how digital forensic copies are stored and used.

The EU has undergone similar changes to due process and privacy protection regulations, with the GDPR being the most prominent. This regulation places severe restrictions on the control and storage of private data, hence privacy protection within the EU. The surveillance and collection of data by steam of digital surveillance are to be conducted in a subsiding core/ essential to protection of frivolous rights.[18]

On the one hand, the EU courts have strengthened the protection of the fundamental rights of individuals regarding the protection of personal data and privacy, on the other hand, have restricted the regulation of the admissibility of digital evidence. In "*La Quadrature du Net v. France"*, [19] CJEU found that the general and indiscriminate retention of communication data by the state violates the fundamental right to privacy and data protection. In "*Prokuratuur v. H.K."*, [20] the CJEU stated that the right to access telecommunications data is of individuals but only after having been subject to prior independent scrutiny. In "*Bundesrepublik Deutschland v. SpaceNet AG"*, [21] court confirmed that general and indiscriminate data retention is contrary to EU law. In "*Privacy International v. Secretary of State for Foreign and Commonwealth Affairs"*,[22] the court stated that there are means to ensure privacy in relation to data protection. In "*Facebook Ireland Ltd v. Schrems (Schrems II)"*,[23] the CJEU targeted the use of data protection in the case of cross border data transfers. In "*Ministerio Fiscal v. Consejo General del Poder*

[16] *HiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019)
[17] *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014)
[18] Claire Laybats & John Davies, "GDPR" 35 *Bus. Info. Rev.* 81 (2018)
[19] ECLI:EU:C:2020:791
[20] ECLI:EU:C:2021:152
[21] ECLI:EU:C:2022:702
[22] ECLI:EU:C:2020:790
[23] ECLI:EU:C:2020:559

Judicial",[24] court stated in relation the access to the data of electronic communication that is of paramount importance that there are judicial control and proportionality. All of the above cases confirm and exemplify the rights given by the EU to individuals and the protection of personal data.

The growth and advancements of digital forensic evidence is proof of the synergy of criminal procedure, technology and constitutional law. While public trust upon digital evidence to improve law enforcement investigation is justified, there are privacy, surveillance, and justice concerns that arise due to the unreliable nature of forensic evidence.

International legal approaches to digital evidence are based on a balancing of evidence, privacy and procedural fairness, with two dominant models in the U.S. and the European Union. The Federal Rules of Evidence (FRE) are the main source of admissibility rules in the United States. The threshold of relevance is set by Rules 401–403 and prejudicial or misleading digital evidence is barred, and Rule 901 is a critical requirement of authentication, which requires proof that digital evidence (e.g., email, metadata, logs) is what it claims to be.[25] Notably Rules 902(13) and 902(14) have modernised the rules of evidence, introducing the concept of self-authentication in documentary evidence and data copied from electronic devices, lessening the need for expert evidence. Complementing evidentiary rules, statutes like the Electronic Communications Privacy Act (ECPA) govern government access to electronic communications, and the Computer Fraud and Abuse Act (CFAA) makes it a crime to breach digital systems' security often resulting in digital evidence in prosecution. These statutory safeguards are complemented by the Fourth Amendment of the United States Constitution, which provides a warrant requirement for searches and seizures of electronic devices, as established in the recent judicial decisions that have been given, and continue to be issued, to give electronic data its own class of privacy interests.[26]

The EU has a more privacy-oriented and coordinated approach to digital evidence, by contrast. The GDPR serves as a foundational principle by placing rigor and strictures on the processing, transfer and admissibility of all personal data, including digital evidence,

[24] ECLI:EU:C:2018:788
[25] Paul Reedy et al., "Digital Evidence" in *Interpol's Forensic Science Review* 393, (2017), https://doi.org/10.1201/ebk1439826584-9
[26] *Ibid*.

and regulates evidence collection with the principles of lawfulness, proportionality, and purpose limitation. The E-evidence Regulation aims to overcome the jurisdictional difficulties in cyberspace by allowing requests from law enforcement authorities of a Member State to the service provider of another Member State to provide electronic evidence directly to the requesting state. Furthermore, the ECHR, especially Art. 8 (right to privacy), provides protection for the right to privacy and restricts state monitoring and data gathering, which impacts the way digital evidence may be collected and utilized in court proceedings.

In addition to supranational instruments, EU Member States have a variety of national procedural laws and EU directives that control evidentiary standards, creating a semi-harmonized, yet diverse legal framework. Domestic laws have been adopted for issues of admissibility, chain of custody and forensic standards for digital evidence, with directives laying down baseline obligations, particularly in the area of cybercrime and data retention. This is a multi-layered approach as compared to the more uniform approach in the United States, with the EU system placing more emphasis on data protection and fundamental rights as opposed to evidentiary admissibility and law enforcement efficiency. These frameworks, when taken together, show the worldwide conflict between justice and the protection of individual freedom in an era of algorithmic and data-based adjudication.[27]

The National Crime Records Bureau has reported a steep rise in cybercrimes registered in India in the past year, as delineated under following table.[28]

Year	Cybercrime Cases Registered (Rajasthan)
2018	1,400
2019	2,150
2020	3,350
2021	4,800
2022	6,900

[27] Zeno Geradts, "Forensic Digital Evidence' in *Forensic Evidence Management* 141, (2017), https://doi.org/10.4324/9781315154916-12.

[28] Indiastat, *Cyber Crimes Data – Rajasthan, available at Cyber Crimes Data, https://www.indiastat.com/rajasthan-state/data/crime-and-law/cyber-crimes* (last visited Apr. 11, 2026).

2023	9,200
2024	14,500 (incl. complaints via cyber portals)
2025	18,700
2026	21,000 (estimated)

Source:- India *Cyber Crimes Data – Rajasthan, available at Cyber Crimes Data*

The use of digital forensic evidence has also noted that there are issues with the legal and institutional frameworks in India. The issues include a lack of sophisticated legal forensic evidence, a lack of legal forensic evidence, a lack of evidence, and a lack of evidence to support a claim that legally supports the right to privacy.[29]

In India, the advent of the legal recognition of electronic records began with enactment of the IT Act, 2000, which made electronic documents & digital signatures legally valid. The courts & legislature have, with the passage of years, provided other procedural methods to control the admissibility of digital evidence.

Although digital evidence has significantly increased and is relied on in proceedings, courts have also noted the possibility and risk of manipulation and fabrication. Digital evidence, when edited, altered, or otherwise manipulated, may show no evidence of an alteration and as a result it may still be reliable. As to this fact, evidentiary reliability has created the need for strict procedural protection (chain of custody, forensic hash creation, and certificate issuance).

Since digital forensics develops alongside most contemporary law enforcement agencies' investigative technologies, it is important to discuss both at the same time. Digital forensics is the discipline concerned with the process for identification, preservation, analysis, & presentation of electronic data in way that would enable its presentation in a court's legally acceptable manner. The growing presence of digital technology in daily living has also resulted in greater volumes of data created from digital communication, online transactions, surveillance technology, and digital personal devices. As a result, digital evidence is at the core of most modern-day criminal investigations, including but not limited to email and chat communications, GPS information, server logs, video

[29] C. Michael Bowers, "The Use of Digital Imaging in Human Identification and Crime Scene Analysis" in *Forensic Dental Evidence* 297 (2011), https://doi.org/10.1016/b978-0-12-382000-6.00016-0.

recordings from CCTV systems, and digital data of transactions. The scope of modern forensics in recovering and interpreting evidence is vital to the field of criminal justice.[30]

When conducting a digital forensic investigation, there are a number of systematic steps taken to capture and clear the evidential value of electronic records. Such steps include finding potentially relevant digital sources, forensic imaging for preservation of the data, examining and analyzing digital objects, & presenting findings before a court in an intelligible and verifiable way. Given the possibility that the court may want to examine the digital evidence, it is important that each of the procedures & steps are done in accordance with the procedures that the court considers. In outcome-based investigations, digital evidence must be handled close to the actual value, since losing the value of electronic data can affect the value of data during the trial.[31]

Even though this case was adjudged before the current framework of analysis, it underscored the significance of electronic evidence for the first time in criminal prosecutions and how it illustrated the value of digital evidence for investigative agencies to reconstruct criminal networks & associated communications.

A primary challenge of assessing digital evidence is the nature of electronic data itself. Unlike physical evidence, digital records are not present, and, at the same time, can be present on several devices, networks, and servers. Using sophisticated software, digital files can be changed or altered, and without leaving evidence of these actions. For this reason, forensic investigators have to use advanced techniques, such as forensic imaging, metadata analysis, hash value analysis, and variations of digital data integrity verifiers, to ensure integrity.

A key element of digital forensic investigations is the international scope of digital data. In the digital world, relevant data and digital evidence on a target may be stored on servers beyond the physical borders of the authorities investigating the case. Because of the nature of data storage and data processing in cloud computing, international tech companies, and global networks, data is stored at different locations around the world.[32]

---

[30] Michael M. Losavio et al., "Boundary Conditions for the Digital Forensic Use of Electronic Evidence and The Need for Forensic Counter-Analysis" in *IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)* (2011), https://doi.org/10.1109/sadfe.2011.2

[31] Shahlaa Mashhadani et al., "Identification and Extraction of Digital Forensic Evidence from Multimedia Data Sources using Multi-algorithmic Fusion" in *5th International Conference on Information Systems Security and Privacy* (2019), https://doi.org/10.5220/0007399604380448

[32] *Supra* note 13.

The ease of digital connectivity has also opened up new avenues for financial crimes. Evidence of electronic records has proven to be invaluable. There is more reliance on transaction records, IP logs, geo-fencing, and other layers of communication to support the offenders' patterns. As to this, cyber-crime units and digital forensic labs are becoming a huge and important part of law enforcement.[33]

Thus, the authorities in a digital forensic investigation must not violate the privacy of the individuals in exercising their given discretion. Relationship between privacy rights and digital evidence is complex. In US, the judicial branch has pointed out that digital devices and their data can and should be afforded an added layer of constitutional protection, especially regarding searches and seizures.

Apart from US, EU established the GDPR in order to legally protect data privacy and digital rights. The GDPR contains a set of rules that, from a legal standpoint, simplifies the framework regarding data collection, data storage, and data processing (to include strict regulation on the collection, storage and processing of personal data) of which there are principles such as DPPL, transparency, and data minimization. European courts have repeatedly said that the collection and processing of data must have a purpose that is legally justified in order to protect fundamental human rights that are at stake.

2. REVIEW OF LITERATURE:

1. Palmer (2026)[34], their study outlines a comprehensive and anticipatory analysis of the newly emerging functions of digital forensics. Study indicates that digital forensic science should not be confined only to the realm of post-crime analysis; it should form part of the core structures and systems of processes in the civil and organizational justice system in order to facilitate investigative processes and comfort organizational risk structures. According to Palmer, the digital world has changed the way data is received and analyzed. These new methods of crime forensic analysis have made investigations of data more complicated. Today's system of digital forensics has not only disrupted traditional forms of forensics but has also made it more complicated, and has also made evidence analysis and collection more complex. Today's forensics requires a combination of more sophisticated techniques and an application SD focus.

[33] Ivan Prysiazhniuk, "Use of digital evidence in criminal process: some issues of right to privacy protection"

[34] Palmer "Unlocking the Potential of Digital Forensic Investigations".

2.Wales (2026),[35] claims in their studies that he has made a more significant contribution to the body of knowledge by offering a more scientific and evidence-based perspective of digital forensic science. The study contends that he has not observed a more widespread increase in the application of digital evidence in criminal trials when compared to the level and standard of forensic evidence. This may demonstrate the high evidentiary value of digital evidence. There is a high degree of fragmentation and limited scientific methods that are not empirically based or tested. In the study, Wales states that a high percentage of forensic techniques are used without any control and empirically based validation, and he suggests that this lack of control and empirical validation should be a concern in relation to the standardization of quality digital evidence. The study argues that in order for digital evidence to be of the same quality and standard, it should be empirically derived, tested, and verified and the same should be true for the standardization of quality.

3. Sunhare and Shaikh (2026),[36] say his studies provide a Focused contribution for forensic analysis of social media crime. The rapid pace of social media related crimes continues to grow. The authors name a plethora of crimes committed using social media. These crimes include, but are not limited to, identity fraud, cyber stalking, social media fraud, online financial crimes, and harassment. The authors are right to say that in such social media crimes, evidence exists within the custodial limits of manipulated, deleted, or modified evidence within an online storage network. The rapid pace of social media related crimes continues to grow. The authors intersect the large amounts of evidence, the different kinds of evidence, the various sources of evidence, and the time changing evidence for the complexity of the digital evidence of these crimes.

4. Roslan (2025),[37] said in the research studies a new standard contribution and paradigm by saying that inclusively to secure the authenticity and integrity of digital evidence of social network crimes without the complication of new technology and evidence crimes, Blockchain in digital crimes and social network investigators can provide a positive impact and evidence of multiple digital crimes. The author talks about the extent of the protection of the integrity of authentic evidence of digital means for the protection of the integrity of evidence.

---

[35]Wales (2026), *"A Research-Focused Framework for Empirical Method Validation in Digital and Multimedia Evidence,"*

[36]Sunhare and Shaikh (2026), *"Digital Forensic Framework for Social Media Crime Investigation using Authentication Technique to Preserve Digital Evidence Integrity,"*

[37] Roslan (2025), *"Investigating Digital Evidence Authenticity in Blockchain-Based Forensic Investigation Environments,"*

5. Rekha and Sudha (2025),[38] said in their studies focus on the challenges posed by emerging technologies like the Internet of Things (IoT). They argue that traditional forensic tools are inadequate to handle the complex, distributed, and heterogeneous nature of IoT-generated data**.** The study proposes a blockchain-assisted framework that ensures secure collection**,** preservation, and transmission of digital evidence, thereby improving its integrity and reliability. At the same time, the authors highlight the need for more advanced forensic tools capable of managing large-scale digital environments.

6. Bharati and Bawiskar (2024)[39] said in their studies there is heavy digital documentation of transgressions because of the increased use of mobile devices and other digitally communicative devices. As the authors inform the readers, a piece of digital evidence can have many problems in regard to acceptance, mainly the issues associated with authenticity of said evidence or injury to the evidence or the evidence chain, or issues associated with the negligence of custodians of digital evidence, standard forensic, & legal knowledge of the custodians to handle the evidence in a manner that is protective of the integrity of the evidence.

7. Caser (2024) [40], said in their studies focuses on the evolving nature of cybercrime and the corresponding evidentiary challenges faced by law enforcement agencies. It highlights the growing sophistication of cybercrime, which is making it harder to gather and hold digital evidence, whether it's ransomware, social engineering, or attacks on critical infrastructure. The report also focuses on the increased role of cross-border cooperation and coordinated investigations, where cybercrime often crosses national boundaries. Moreover, it highlights the burden of operational duties on judicial and investigative units, its growing involvement in cybercrime investigations and multilateral investigation mechanisms, thus promoting the need for harmonized evidentiary standards and strengthening institutional capacities.

8. ENISA (2024)[41] offers a broad characterisation of the EU cyber security and digital evidence scenario. It highlights major threats including ransomware, distributed denial of service (DDoS) attacks and data breaches, as well as examining the involvement of various

[38] Rekha and Sudha (2025), *"Blockchain-Assisted Digital Forensic Framework in the IoT Paradigm,"*
[39] Rahul Bharati et al., "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings"
[40] Eurojust, *Annual Report 2024: Cybercrime*, Eurojust (2024)
[41] Assaf Kerret et al., "Blockchain-Based Frameworks for Digital Evidence Management

threat actors, including state-sponsored threat groups and cybercriminal organizations. The report notices the growing amount and complexity of digital evidence from cyber incidents and emphasises the need for preparedness, incident response and regulatory frameworks to deal with this digital evidence effectively. It also highlights structural issues, such as skills shortages and harmonisation of practices at the Member State level, underscoring the need for coordinated policy and technical solutions for the reliability and admissibility of digital evidence.

9. Kerret et al. (2023)[42] focus on the technical and procedural difficulties in dealing with electronic evidence in cybercrime investigations while highlighting the ever-expanding body of scholarship surrounding digital evidence management. The authors raise concerns regarding data integrity, chain of custody and admissibility, especially in the presence of decentralized and encrypted systems. One of the main findings of the study is the role of emerging technologies, particularly blockchain, in providing secure storage and verifiable audits of digital evidence, ensuring its tamper-proof nature. By proposing a distributed ledger-based framework, the study argues that evidentiary reliability and cross-border cooperation can be significantly enhanced, thereby addressing longstanding concerns regarding authenticity and manipulation in digital forensic processes.

10. Weifeng Xu and Dianxiang Xu (2022)[43], said in their studies examines the presentation of digital evidence and how it could be structured for easier comprehension and potentially different arrangements. The authors focus on knowledge graphs to better manage digital evidence. Knowledge graphs could simplify management of large electronic datasets for the purposes of legal investigations and court cases. Xu and Xu identify digital forensic investigations, from different cloud servers and networks, including multiple mobile devices or documents and spanning large datasets. In their opinion, and for a court to adequately interpret the digital evidence or datasets, the evidence would have to be presented in a non-traditional style.

[42] European Union Agency for Cybersecurity, "ENISA Threat Landscape" 2024, *ENISA* (2024)
[43] Weifeng Xu & Dianxiang Xu, "Visualizing and Reasoning about Presentable Digital Forensic Evidence with Knowledge Graphs"

11. Dr. Muhammad Ramzan (2022)[44], said in their studies digital and forensic evidence is the only type of evidence that is objective and scientifically clear in relation to the criminal activity that has occurred, unlike forensic evidence or other alternative digital forensic evidence that relies on eyewitness accounts/forensic accounts. While the reliance on eyewitness accounts has traditionally dominated the field of criminal evidence, The author reviews the latest amendments in legislation & recent judicial approach to the more recently developed forensic and digital evidence.

12. Tanmayee Tilekar (2020) [45] said in their studies unique challenges and growing significance of IOT devices as evidence in digital forensics. IOT devices include smart home systems, wearables , and smart appliances, and they can generate a large amount of data which can be used for criminal investigations. Tilekar discusses data collection and analysis challenges related to the legal and technical aspects of these devices.

13. Robin Verma, Jayaprakash Govindaraj, Saheb Chhabra, and Gaurav Gupta (2019) [46] said in their studies new instance of advanced digital forensic frameworks using machine learning and a privacy protection framework. The authors claim that one of the shortcomings of current digital forensic methodologies is that they require numerous manual reviews of extensive and burdensome datasets.

14. Sachowski (2019)[47], said in their studies innovative digital forensic framework, DF 2.0. This framework integrates new automation and predictive algorithm technologies to enhance an investigator's ability to develop relevant digital evidence. At the same time, the framework's privacy protection technologies facilitate the protection of unrelated sensitive personal data. The authors of the paper acknowledge that the digital data that is reviewed and analyzed poses significant ethical and legal challenges to the practice of digital forensic investigations.

[44] Dr Muhammad Ramzan, "Forensic and Digital Evidence be used as Substantial Evidence in Criminal Cases, an Effective Alternative of Ocular Account: Evaluation in the Light of New Amendments. What are the Requirements of Admissibility and Reliability of Digital and Forensic Evidence?"
[45] Tanmayee Tilekar, "The Conceivability And Admissibility Of Forensic Evidence from IoT Devices in Digital Forensics"
[46] Robin Verma et al., "DF 2.0: An Automated, Privacy Preserving, and Efficient Digital Forensic Framework That Leverages Machine Learning for Evidence Prediction and Privacy Evaluation"
[47] Jason Sachowski, "Digital Evidence Management"

15. Gavin Hales and Ethan Bayne (2019)[48]**,** said in their studies how digital forensics can be improved using visualization technology. The authors mention that during digital forensic examinations, investigators are faced with a huge amount of data, and finding pertinent data can be a challenging task. This study focuses on the visualization techniques that assist investigators with the rapid triage of digital evidence by capturing valuable insights with regard to patterns, anomalies, and relationships in a dataset.

16. Geradts (2017)[49] said in their studies that investigators can cut the time needed to do a thorough forensic analysis by focusing their analysis on pertinent evidence through the visualization of networks, communication logs, and file structure. The authors note that the value of visualization tools is even more enhanced in the initial phases of investigations when the investigators must make quick decisions on the devices or files that could store vital evidence.

17. Soowoong Eo, Wooyeon Jo, Seokjun Lee, and Taeshik Shon (2016)[50] said in their studies mobile forensics' challenges in the context of evidence that can be obtained from mobile devices. The authors focus on the challenges that investigators face regarding the extraction, preservation, and analysis of mobile data. Eo, Jo, Lee, and Shon stress the importance of mobile forensic investigators using consistent methodologies and having an established, documented chain of custody when collecting mobile data.

18. Richard Boddington (2016)[51] said in their studies some of the complications related to the collection and evaluation of digital evidence. In his book chapter, Richard Boddington elaborates on some elements of digital forensic examination and how effective each of the elements is. With the rapid development of technology, there is a rapid increase in the amount of data, and there is increased use of encrypted data. As technology develops, digital storage also develops, and because of this, investigators must go through large amounts of data in order to find the evidence.

[48] Gavin Hales & Ethan Bayne, "Investigating Visualisation Techniques for Rapid Triage of Digital Forensic Evidence"
[49] Zeno Geradts, "Forensic Digital Evidence"
[50] Soowoong Eo et al., "Ensuring the Admissibility of Mobile Forensic Evidence in Digital Investigation"
[51] Richard Boddington, "Current and Future Challenges Confronting the Use of Digital Evidence"

19. Dinkar (2015)[52], said in their studies readers to develop methodologies that focus on the improvement of credibility and admissibility regarding mobile forensic evidence so that more mobile data can be utilized in legal matters.

20. Oriola Sallavaci and Carlisle George (2013)[53] said in their studies growing legal framework of expert testimony to digital forensics. Their article discusses how judicial systems assess expert opinions on digital forensics & role of transparency and reliability in science. Digital forensics experts must be specific regarding the methods, tools, and analyses employed during their investigations, as this will help the courts assess credibility. The authors, by describing the procedural changes in the law concerning the role of digital forensic experts in the evolving legal landscape, help clarify the professional and legal standards digital forensics practitioners must meet to ensure their testimony is judicially accepted.

21. C. Michael Bowers (2011)[54] said in their studies use of technologies in forensic imaging. The author discusses the use of imaging in documenting crime scenes, analyzing evidence, and aiding in the identification of individuals. The Forensic Documentation Initiative focuses on the use of high-quality photographs and captures the skin of crime scenes in three dimensions.

22. Bianchi & Pollitt (2006)[55] said in their studies use of advanced imaging tools to assist investigators in the identification of victims & perpetrators of a crime, & reconstruction of faces. The assimilation of modern forensic technologies into forensic imaging enhances the precision and reliability of investigators' aid in preserving and visually reproducing evidence.

[52] V. R. Dinkar, "Forensic scientific evidence: problems and pitfalls in India"
[53] Oriola Sallavaci & Carlisle George, "Procedural aspects of the new regime for the admissibility of expert evidence: what the digital forensic expert needs to know"
[54] C. Michael Bowers, "The Use of Digital Imaging in Human Identification and Crime Scene Analysis"
[55] Robert P. Bianchi & Mark Pollitt, "Digital Evidence"

3. RESEARCH GAPS:

1. There are very few studies that have empirically examined how digital evidence is used in criminal justice processes, especially at the state level, despite the growing importance of digital evidence in criminal investigations and prosecutions in India.

2. Most of the studies available concentrate either on the technological progress of digital forensics or the doctrinal studies of the legal provisions, leaving an evident gap at the interface of law, forensics, and procedures.

3. There have been cases of judicial pronouncements that have played a role in the development of the law concerning electronic evidence poring over the gaps; and drawbacks beyond the realms of evidence and the law of evidence, like the challenge of authenticity, substantiating the element of integrity, the chain of custody, and the reliability of the evidence in criminal adjudicatory processes, remain under-evaluated.

4. More critically, the legal framework of BSA, 2023, of the developing, and the still evolving, digital evidence of admissibility and certification, have insufficient legal concern.

There is, then, a large gap in the absence of judicially or financially substantiated processes and practical challenges where laws and policies will most likely be of, at best, little value. Most attempts at reforming criminal justice in India are focused on either procedural or sentencing issues, leaving the issues of digital evidence and the implications for the rule of law, justice, and individual freedoms unaddressed. The most important gap that this study intends to fill, in this context, is the complete absence of applied and cross-disciplinary studies.

4. STATEMENT OF THE RESEARCH PROBLEM:

The rapid advancement of technology in the spheres of social networks, economics, and communications has significantly impacted how criminal investigations are carried out as well as how criminal trials are structured. Devices used in everyday activities, such as cell phones, computers, and even surveillance and cloud storage technology, generate endless streams of digital information. This information can potentially be used as evidence in most criminal activities. In this aspect, digital evidence is increasingly playing a role in the detection, investigation and prosecution of crimes for law enforcement.

The Internet and smart phone use has expanded quickly in the state and has led to an increase in cyber crimes such as online fraud, digital financial crimes, and identity theft. The growing digitization has left electronic and forensic evidence playing an important role in the criminal investigation in Rajasthan and has also created a concern about its admissibility, reliability and the protection of individual privacy in the criminal justice system.

But digital and forensic evidence is growing in importance and its use in criminal proceedings has posed a number of legal and practical challenges. Unlike conventional evidence, digital information can be altered, duplicated, or deleted with little or no trace. This presents an overwhelming number of challenges in evidence collection and processing to investigators, forensic specialists, and judges. The collection of digital evidence can be compromised by the lack of standard forensic practices, poor management of the evidence collection process, and loss of control in the evidence collection process, all of which significantly reduce the reliability of digital evidence used in court.

5. SIGNIFICANCE OF THE STUDY:

With regard to the rapidly evolving nature of the interface between developing technologies and different systems of criminal justice, the study becomes necessary. Given the digitalization of almost every human activity, a significant part of which can also be relevant for criminal acts, Digital forensic evidence has a critical role to play in today's law enforcement and judicial processes.

The purpose of the research is the academic contribution to the area of digital and forensic evidence as to Rajasthan, India & way they interact within the context of criminal proceedings. Since digital evidence is different to traditional evidence, it is essential to investigate the complexities of digital evidence and challenge its manipulation. Understanding the gaps in the principles of law governing the admissibility and reliability of electronic evidence provides clarity on how this evidence can meet scientifically legal standards.

6. RESEARCH OBJECTIVES:

1. To evaluate the admissibility, reliability, and evidentiary value of digital forensic evidence in criminal trails.

2. To analyze the existing framework governing digital forensic evidence to assess admissibility, reliability and evidentiary value related provision in criminal trial in India.

3. To study judicial response towards admissibility, reliability, and evidentiary value of digital forensic evidence in criminal trails.

4. To compare foreign laws related to digital forensic evidence with Indian laws to derive best practices.

5. To empirically assess the perspective of stakeholders regarding the use, reliability and challenges of digital forensic evidence in criminal trials in Rajasthan.

6. To propose evidence based legal and policy reforms aimed at strengthening the admissibility, reliability, and accountability of digital forensic evidence in criminal justice administration.

7. RESEARCH QUESTIONS:

1. To what extent is digital forensic evidence admissible and reliable in criminal trials?

2. What is the existing legal framework governing digital forensic evidence in criminal trials in India?

3. Whether Indian judiciary goal has been positive towards admissibility, reliability, and evidentiary value of digital forensic evidence in criminal trials?

4. Whether the best practices relating to digital evidence in foreign jurisdictions are reflected in the Indian legal framework?

5. What are the stakeholders perspective regarding the use and challenges of digital forensic evidence?

6. What legal and policy reforms are necessary to ensure effective and fair use of digital forensic evidence in criminal trials?

8. RESEARCH HYPOTHESES:

H1: There exist a significant gap between the legal framework governing digital forensic evidence and its flawed implementation, adversely affecting its admissibility, reliability and evidentiary value in criminal trials.

H2: The effectiveness of digital forensic evidence in criminal trials is significantly influenced by Legal, infrastructural, financial and procedural barrier in state of Rajasthan.

H3: Judiciary in India faced challenges in relation to admissibility, reliability, and evidentiary value of digital forensic evidence in criminal trails.

9. RESEARCH METHODOLOGY:

The aim of this study is to better understand the digital forensic legal framework. This includes its implementation in criminal cases in the state of Rajasthan. This study combines empirical legal research with doctrinal legal research to meet its aim. Doctrinal research alone will not be helpful in capturing challenges presented to the legal forensic framework. This study incorporates the use of both structured questionnaires and interviews, in order to provide insight for legal and forensic case practitioners. It will also provide an analysis of judicial decisions, statutory provisions, and a framework for comparative legal analysis. Admissibility and scope of digital evidence will be explained in a preliminary analysis.

Study Area

This research aims to cover the state of Rajasthan pertaining to the selected districts of Jaipur, Alwar, Bharatpur, and Jodhpur. This study shall include judicial institutions like the District and Sessions Courts and Rajasthan High Court, Supreme Court, etc., where the issues regarding admissibility, dependability, and the evidentiary worth of digital evidence shall be tackled.

Target Population

This research encompasses the main stakeholders of the criminal justice system, inclusive of police personnel, lawyers, and former judges. Former judges and lawyers shall offer perspectives on aspects of evidence, whereas police personnel shall provide input on matters of evidence and the investigative process.

Method of sampling

This study intends to employ a non-probability sampling technique. The purposive sampling technique shall be adopted to ensure the adequate representation of these stakeholders, such as police personnel, lawyers, and former judges in the state of Rajasthan. The technique of

purposive sampling shall be employed to ensure the selection of the most qualified and experienced participant.

Sample Size

This research shall encompass total of 500 participants comprising police personnels, advocates, & former judges.

Data Analysis

In this qualitative study, thematic analysis shall be employed to analyze the participants' responses to the open-ended questions in the interviews and questionnaires. This shall help to elucidate the emerging patterns and dominant themes. To examine the trends pertaining to the use, admissibility, reliability, and evidentiary value of digital evidence in criminal trials.

Types of Data

A. Primary Data – I will collect primary data using structured questionnaires and semi-structured interviews of police personnel, lawyers, and former judges.

B. Secondary Data - I will collect secondary data from statutory laws, judicial rulings, law commission reports, policy papers, and scholarly writings. I also reviewed forensic reports and comparative legal literature concerning digital evidence in India, the USA, and the EU.

10. SCOPE OF THE STUDY:

This study focuses on the role and significance of digital forensic evidence in criminal trials within the Indian legal system. It examines the existing legal framework governing digital evidence, particularly under the IT Act, 2000 and the BSA, 2023. The research explores the entire process of handling digital evidence, including its collection, preservation, and presentation before courts. It further analyses critical issues such as admissibility, reliability, and evidentiary value of digital evidence in judicial proceedings. An empirical component is included through responses gathered from police officials, advocates, and retired judges to understand practical perspectives. The study also investigates the real-world challenges faced by investigating agencies and courts, including procedural, technical, and infrastructural limitations. Hence, the research aims to provide meaningful suggestions and reforms to improve the effective use and acceptance of digital forensic evidence in the criminal justice system.

11. LIMITATIONS OF THE STUDY:

1. The study is confined to the legal and procedural aspects of digital forensic evidence and does not cover detailed technical analysis of forensic tools and software.
2. It is limited geographically to Rajasthan, so the findings may not be applicable to other states or countries.
3. The study relies on secondary data and limited empirical inputs, which may not fully represent all stakeholders such as police officials, advocates, retired judges.
4. There may be lack of access to confidential or sensitive case data, which limits in-depth empirical analysis.
5. The study may face limitations in availability of updated statistical data on digital evidence usage in Rajasthan courts.

12. EXPECTED OUTCOMES:

The study hopes to achieve a complete understanding of digital forensic evidence admissibility, reliability and evidentiary value in criminal trails. The research is likely to illuminate practice and procedural limitations of current evidence frameworks and identify some of the best practices from the US and EU. The empirical research study is likely to expose stakeholder perceptions of digital evidence usage and offer recommendations to improve investigative processes, evidence, & clarity of privacy protections in the criminal justice system.

13. RESEARCH TIMELINE:

S.NO.	Research Phase	Activities	Time period
1.	Background Study & Literature Review	Extensive review of books, journals, articles, and case laws related to the research topic. Identification of research gap and refinement of research objectives.	Jan , 2026
2.		Finalization of research methodology, preparation of research tools such as	July, 2026

	Research Design & Methodology	questionnaires/interview schedules, and approval from supervisor	
3.	Data Collection	Collection of primary and secondary data through surveys, interviews, case studies, reports, and legal documents	Dec, 2026
4.	Data Analysis & Interpretation	Systematic analysis and interpretation of collected data using qualitative and quantitative methods**.**	June , 2027
5.	Drafting of Chapters	Preparation of research chapters including introduction, literature review, methodology, analysis, and findings**.**	Dec , 2027
6.	Review & Finalization	Revision of thesis based on supervisor's suggestions and incorporation of corrections	Feb , 2028

14. BIBLIOGRAPHY:

- "Increase In Cyber Crimes" *Press Information Bureau* (2024), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505.
- C. Michael Bowers, "The Use of Digital Imaging in Human Identification and Crime Scene Analysis" in *Forensic Dental Evidence* 297 (2011), https://doi.org/10.1016/b978-0-12-382000-6.00016-0.
- Claire Laybats & John Davies, "GDPR" 35 *Bus. Info. Rev.* 81 (2018), https://doi.org/10.1177/0266382118777808.
- Dr. Muhammad Ramzan, "Forensic and Digital Evidence be used as Substantial Evidence in Criminal Cases, an Effective Alternative of Ocular Account: Evaluation in the

Light of New Amendments. What are the Requirements of Admissibility and Reliability of Digital and Forensic Evidence?" 2022 *SSRN Elec. J.*, https://doi.org/10.2139/ssrn.4021315.

- Gavin Hales & Ethan Bayne, "Investigating Visualisation Techniques for Rapid Triage of Digital Forensic Evidence" in *HCI for Cybersecurity, Privacy and Trust* 277 (2019), https://doi.org/10.1007/978-3-030-22351-9_19.
- Ivan Prysiazhniuk, "Use of digital evidence in criminal process: some issues of right to privacy protection" 5 *Visegrad J. on Hum. Rts.* 81, (2023), https://doi.org/10.61345/1339-7915.2023.5.11.
- Jason Sachowski, "Digital Evidence Management" in *Implementing Digital Forensic Readiness* 24, (2019), https://doi.org/10.4324/9780429441363-3.
- Michael M. Losavio et al., "Boundary Conditions for the Digital Forensic Use of Electronic Evidence and The Need for Forensic Counter-Analysis" in *IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)* (2011), https://doi.org/10.1109/sadfe.2011.2.
- Oriola Sallavaci & Carlisle George, "Procedural aspects of the new regime for the admissibility of expert evidence: what the digital forensic expert needs to know" 5 *Int'l J. Elec. Sec. & Digit. Forensics* 161 (2013), https://doi.org/10.1504/ijesdf.2013.058645.
- Rahul Bharati et al., "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings" 2024 *SSRN Elec. J.*, https://doi.org/10.2139/ssrn.4896874.
- Richard Boddington, "Current and Future Challenges Confronting the Use of Digital Evidence" in *Emerging Forensic Tools for Locating and Analyzing Digital Evidence 1671*, https://doi.org/10.4018/978-1-4666-9591-7.les3 (last visited Mar. 8, 2026).
- Robert P. Bianchi & Mark Pollitt, "Digital Evidence" in *The Forensic Laboratory Handbook* 79 (2006), https://doi.org/10.1385/1-59259-946-x:79.
- Robin Verma et al., "DF 2.0: An Automated, Privacy Preserving, and Efficient Digital Forensic Framework That Leverages Machine Learning for Evidence Prediction and Privacy Evaluation" 2019 *J. Digit. Forensics Sec. & L.*, https://doi.org/10.15394/jdfsl.2019.1606.
- Shahlaa Mashhadani et al., "Identification and Extraction of Digital Forensic Evidence from Multimedia Data Sources using Multi-algorithmic Fusion" in *5th International Conference on Information Systems Security and Privacy* (2019), https://doi.org/10.5220/0007399604380448.

- Soowoong Eo et al., "Ensuring the Admissibility of Mobile Forensic Evidence in Digital Investigation" 26 *J. Korea Inst. Info. Sec. & Cryptology* 135 (2016), https://doi.org/10.13089/jkiisc.2016.26.1.135.
- Tanmayee Tilekar, "The Conceivability And Admissibility Of Forensic Evidence from IoT Devices in Digital Forensics" *Digit. Forensics (4n6) J.* 53 (2020), https://doi.org/10.46293/4n6/2020.02.02.10.
- V. R. Dinkar, "Forensic scientific evidence: problems and pitfalls in India" 3 *Int'l J. Forensic Sci. & Pathology* 79 (2015), https://doi.org/10.19070/2332-287X-1500020.
- Weifeng Xu & Dianxiang Xu, "Visualizing and Reasoning about Presentable Digital Forensic Evidence with Knowledge Graphs" in *19th Annual International Conference on Privacy, Security & Trust (PST)* (2022), https://doi.org/10.1109/pst55820.2022.9851972.
- Zeno Geradts, "Forensic Digital Evidence" in *Forensic Evidence Management* 141 (2017), https://doi.org/10.4324/9781315154916-12.
- Assaf Kerret et al., "*Blockchain-Based Frameworks for Digital Evidence Management*
- C. Michael Bowers, "The Use of Digital Imaging in Human Identification and Crime Scene Analysis" in *Forensic Dental Evidence* 297 (2011), https://doi.org/10.1016/b978-0-12-382000-6.00016-0.
- Dr. John Varghese, "Electronic form evidence under the Bharatiya Sakshya Adhiniyam, 2023" 2024 *SSRN Elec. J.*, https://doi.org/10.2139/ssrn.4869744.
- Dr. Muhammad Ramzan, "Forensic and Digital Evidence be used as Substantial Evidence in Criminal Cases, an Effective Alternative of Ocular Account: Evaluation in the Light of New Amendments. What are the Requirements of Admissibility and Reliability of Digital and Forensic Evidence?" 2022 *SSRN Elec. J.*, https://doi.org/10.2139/ssrn.4021315.
- Eurojust, *Annual Report 2024: Cybercrime*, Eurojust (2024)
- European Union Agency for Cybersecurity, "*ENISA Threat Landscape" 2024*, *ENISA* (2024)
- Indiastat, *Cyber Crimes Data – Rajasthan, available at Cyber Crimes Data, https://www.indiastat.com/rajasthan-state/data/crime-and-law/cyber-crimes* (last visited Apr. 11, 2026).
- Michael M. Losavio et al., "Boundary Conditions for the Digital Forensic Use of Electronic Evidence and The Need for Forensic Counter-Analysis" in *IEEE Sixth*

International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE) (2011), https://doi.org/10.1109/sadfe.2011.2

- Paul Reedy et al., "Digital Evidence" in *Interpol's Forensic Science Review* 393, (2017), https://doi.org/10.1201/ebk1439826584-9
- Rahul Bharati et al., "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings"
- Rekha and Sudha (2025), *"Blockchain-Assisted Digital Forensic Framework in the IoT Paradigm,"*
- Roslan (2025), *"Investigating Digital Evidence Authenticity in Blockchain-Based Forensic Investigation Environments,"*
- Shahlaa Mashhadani et al., "Identification and Extraction of Digital Forensic Evidence from Multimedia Data Sources using Multi-algorithmic Fusion" in *5th International Conference on Information Systems Security and Privacy* (2019), https://doi.org/10.5220/0007399604380448
- Sunhare and Shaikh (2026), *"Digital Forensic Framework for Social Media Crime Investigation using Authentication Technique to Preserve Digital Evidence Integrity,"*
- Wales (2026), *"A Research-Focused Framework for Empirical Method Validation in Digital and Multimedia Evidence,"*
- Zeno Geradts, "Forensic Digital Evidence' in *Forensic Evidence Management* 141, (2017), https://doi.org/10.4324/9781315154916-12